# ACM/IEEE International Workshop on Security and Privacy Preserving in e-Societies (SeceS'11)

## Final Program

| | Thursday - June 9, 2011 | Friday - June 10, 2011 | Saturday - June 11, 2011 |
|---|---|---|---|
| 09:00 - 09:30 AM | | Session 4 | Excursion |
| 09:30 - 09:45 AM | Registration | | |
| 09:45 - 10:15 AM | Opening Session | | |
| 10:15 - 11:00 AM | Welcome Reception | Coffee Break | |
| 11:00 - 11:30 AM | Session 1 | Session 5 | |
| 11:30 - 12:00 AM | | | |
| 12:00 - 12:30 PM | | | |
| 12:30 - 02:00 PM | Lunch | | |
| 02:00 - 02:30 PM | Session 2 | Panel<br>Social Network Security | |
| 02:30 - 03:00 PM | | | |
| 03:00 - 03:30 PM | | | |
| 03:30 - 04:00 PM | Coffee Break | Coffee Break | |
| 04:00 - 04:30 PM | Session 3 | Student Session | |
| 04:30 - 05:00 PM | | | |
| 05:00 - 05:30 PM | | | |


Workshop Location
Antonine University
Faculty of Engineering
www.upa.edu.lb

Tel.: + 961 5 924 073/4/6 - Fax: + 961 5 924 815
B.P.: 40016 Hadath - Baabda – Lebanon
lt.lg.: 33 50.1653' N, 35 32.1251' E

## Session 1

### Keynote 1 by Alban Gabillon

**Bio**: Alban Gabillon is a Professor in Computer Science at the University of French Polynesia. He has worked for more than 15 years on various areas of Computer Security, including access control, multilevel security, xml security, secure timestamping and protection of geographic data. He has authored or co-authored more than 60 papers published in international journals or international conference proceedings. He is a co-chair of the French working group on Information System Security (GDR I3/SSI)

*Talk: Protection of Geographic Information*

**Abstract:** Many new internet applications use geo-referenced data (maps services, navigation software, vehicle tracking etc.). Securing access to geo-referenced data in location-based services requires the definition of spatially aware access control systems. In this presentation, we define a complete security model for geographic applications. Our model considers dynamic spatial security rules. A spatial dynamic security rule can be activated or deactivated depending on some spatial context. Our model considers also the various existing methods for protecting unauthorized geographic objects. It includes a framework for specifying whether unauthorized objects should be erased, blurred, masked or pixelizated. We sketch the implementation of our model within the framework of a Web Map Service.

*Paper 1 by Nidal Khoury, Pavol Zavarsky, Dale Lindskog and Ron Ruhl.*

*Testing and Assessing Web Vulnerability Scanners for Persistent SQL Injection Attacks*

**Abstract:** Web application security scanners are automated tools used to detect security vulnerabilities in web applications. Recent research has shown that detecting persistent SQL injection vulnerabilities, one of the most critical web application vulnerabilities, is a major challenge for black-box scanners. In this paper, we evaluate three state of art black-box scanners that support detecting persistent SQL injection vulnerabilities. We developed our custom testbed "MatchIt" that tests the scanners capability in detecting persistent SQL injections. The results show that existing vulnerabilities are not detected even when these automated scanners are explicitly configured to exploit the vulnerability. The weaknesses of black-box scanners identified reside in many areas: crawling web pages, input values and attack code selection, user registration and login, analysis of server replies and classification of findings. Because of the poor detection rate, we analyze the scanner's behavior and present a set of recommendations that could enhance the discovery of persistent SQL injection vulnerabilities.

*Paper 2 by David Pergament, Armen Aghasaryan, Jean-Gabriel Ganascia and Stéphane Betgé-Brezetz.*

*FORPS: Friends-Oriented Reputation Privacy Score*

**Abstract:** The Friends-Oriented Reputation Privacy Score (FORPS) system provides a smart and simple way to help end-users managing their privacy in a social network. It aims to prevent a non-desirable propagation of personal sensitive data. FORPS built privacy sensitivity profile by understanding what are the category of themes, the category of objects and the behavioral factors that are important to social network users. FORPS takes fully advantage of knowledge retrieved on social networks, in particular via user friends. More precisely, our approach consists in making a deep analysis of the behavior of somebody who would like to get in touch with a user in order to estimate the risk of potential violation of his privacy information.

## Session 2

### Keynote 2 by Lionel Brunie

**Bio**: Lionel Brunie is full professor at the National Institute of Applied Sciences (INSA) of Lyon, France. After he received his PhD in computer science in 1992 from Joseph Fourier University, Grenoble, France, Lionel Brunie joined Ecole Normale Supérieure of Lyon, France (LIP lab) as assistant professor. His domains of interest were then parallel programming environments, parallel databases and multimedia distributed systems. Since October 1998, Lionel Brunie is full professor in computer science at the National Institute of Applied Sciences (INSA) of Lyon, France. In 1999, Lionel Brunie created INSA e-learning department that he led until 2002. Then he headed the Lyon doctoral school in computer science (300+ registered PhD students). In 2002, Lionel Brunie co-founded the LIRIS lab in which he acted as deputy director in 2006-2007 (the LIRIS lab presently hosts 300 staff and PhD students). In 2007, along with Pr Harald Kosch (Univ. of Passau, Germany), Lionel Brunie created the French-German doctoral college in "Multimedia, Distributed and Pervasive Secure systems" (MDPS). Since then, L. Brunie and H. Kosch jointly head this doctoral college. In 2010, along with Pr Ernesto Damiani (University of Milan, Italy), Lionel Brunie created the French-Italian doctoral college in "Collaborative and Secure Management of Knowledge". These two doctoral colleges, which are managed in close relationship, propose an international coordinated PhD program focused on distributed

systems, multimedia and security. They are based on a joint research program that links the three involved teams. Lionel Brunie leads a research team of 10 permanent researchers and 25+ PhD students specialized in information management in distributed systems and security. His main topics of interest include: data management in large scale and pervasive systems, security and privacy, collaborative multimedia information systems, medical informatics. Lionel Brunie has led numerous national and international research projects; he is the (co-)author of over 180 research papers; he has been member of over 60 scientific conference and workshop committees. More information can be found at: http://liris.cnrs.fr/lionel.brunie/.

### *Talk: Trust and Reputation*

**Abstract:** Trust and reputation are essential ingredients of interpersonal relationships. In our emerging e-society, trust and reputation are equally essential ingredients for successful transactions between businesses.

Trust and reputation are symbolic representations, symbolic attributes associated by one entity to another entity based on their past exchange history [Zucker, 1986]. Trust is based on a personal opinion ("Trust […] is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action" [Gambetta, 2000]"); oppositely, reputation is a common opinion, the opinion of a community about the trustworthiness of an individual or an organization.

However, both concepts refer to the same issue (the confidence in another entity within the context of a given decision) and can cross-fertilize: reputation can be used to determine the trust one party can have in another; oppositely, reputation can be estimated by gathering trust feedbacks from the members of a community.

Open and virtual computing infrastructures (e.g., the Web, peer to peer systems, clouds, mobile pervasive environments, open SOAs, etc.) have triggered a very strong movement of interest for the notions of trust and reputation. Indeed, in such environments, classical security enforcement techniques are no more pertinent as no central server or trusted third party exist that can serve as decision-taking oracle. Reputation and trust then appear as the few alternatives available to establish a rational decision**.**

This talk will be organized in two parts. First, we will define the notion of trust and reputation, and present basic techniques used for computing trust and reputation values in decentralized environments. In a second phase, we will point out and discuss open issues related to trust and reputation in emerging open infrastructures e.g., clouds of services, mobiles systems, B2B e-marketplaces.

### *Paper 3 Nashwa El-Bendary, Aboul Ella Hassanien, Javier Sedano, Omar S. Soliman, Neveen I.Ghali*

### *µTESLA-based Secure Routing Protocol for Wireless Sensor Networks*

**Abstract:** Wireless sensor networks are highly prone to security threats due to resource constraints and the broadcast nature of the transmission medium. Directed diffusion protocol is one of the routing protocols for wireless sensor networks that are not designed with security in mind and are particularly susceptible to different security attacks. In this paper, a secure routing protocol for wireless sensor networks, based on the directed diffusion routing algorithm, is presented. The proposed secure routing protocol uses the µTESLA (micro Timed, Efficient, Streaming, Loss-tolerant Authentication) broadcasting authentication algorithm in order to authenticate the acknowledgement messages sent from the sink to the source nodes for confirming the delivery of the data-event messages. A simulation based performance evaluation for the proposed protocol was conducted against black hole and acknowledgement-spoofing attacks. Simulations show that, compared to the original directed diffusion protocol, the proposed secure routing protocol achieved better event-delivery and event-dropping ratios. However, it resulted higher cost in the mean dissipated energy and average delay in some situations due to acknowledgement and authentication processes for delivered events and also due to the retransmissions of non-acknowledged events.

## Session 3

### Keynote 3 by Ernesto Damiani

**Bio**: Ernesto Damiani is a professor at the Department of Information Technology of the University of Milan, where he leads the Secure Software Architectures Lab (SESAR - http://ra.crema.unimi.it). He is also the Director of the University of Milan's Ph.D. program in Computer Science. Ernesto has held visiting positions at George Mason University, VA (USA), La Trobe University, Melbourne, Australia, and the University of Technology, Sydney, Australia. His research interests include business process representation and metrics, knowledge extraction and processing, secure service-oriented architectures, software process engineering and soft computing. On these topics he has filed international patents with companies like Siemens and British Telecom and published more than 180 refereed papers in international journals and conferences, as well as several books. Ernesto is the Vice-Chair of the IEEE

TC on Industrial Informatics, the Chair IFIP WG on Data Semantics (WG 2.6) and the Vice-Chair of the IFIP WG 2.13 on Open Source Software. Ernesto Damiani has a wide experience is journal editorships, as an Associate Editor of the IEEE Transactions on Service Computing, an Area Editor at the Journal of System Architecture, and as the co-Editor in Chief of the International Journal of Electronic Trade. He serves in the steering committee of other journals, such as the International Journal of Knowledge-Based Intelligent Engineering Systems and International Journal of Technology Enhanced Learning.

*Talk: Protecting the Virtual Infrastructure from Cyber-crime*

**Abstract:** The ongoing merge between Service-Oriented Architectures (SOAs) and the Cloud computation paradigm provides a new global infrastructure based on the integration of services located within company boundaries with those virtualized on the Cloud. An increasing number of organizations, including government agencies, implement their business processes via runtime composition of services made available on the Cloud by external suppliers; also, individuals increasingly use cloud-based services in addition to their local applications to support their everyday work and leisure activities. This scenario is introducing new risks and threats, for sensitive data and requires re-thinking of current data protection methodologies. The talk addresses some cyber-crime and cyber-terrorism issues related to data sharing on the cloud, along with evaluating their impact on traditional security solutions for software and network systems.

*Paper 4 Rony Darazi, Mireia Montanola Sales, Li Weng, Benoît Macq and Bart Preneel.*

*Disparity Guided Exhibition Watermarking for 3D Stereo Images*

**Abstract:** In this paper, a watermarking scheme for 3D stereo images is presented. The target application is 3D Digital Cinema. The watermarking is based on a dependent stereo image coding scheme, where the watermark is embedded in the JPEG2000 decoding pipeline after the inverse quantization and prior to the inverse discrete wavelet transform (IDWT). A perceptual mask is designed to cope with the particularity of the 3D perception and is tuned by the disparity map and the wavelet properties related to the Human Visual System (HVS). In this scheme, the watermark is inherited in the target image during the decoding process and hence, both the reference and the target image in the stereo pair are watermarked. Our results show improvements due to the integration of the 3D visual mask in terms of Structural Similarity Metric (SSM) and Bit Error Rate (BER).

## Session 4

### Keynote 4 by Qutaibah Malluhi

**Bio:** Qutaibah Malluhi has been appointed as the head of the Department of Computer Science and Engineering since in 2006. Before joining Qatar University he was a professor of Computer Science at Jackson State University where he served as a faculty member between 1994 and 2005. During 1995 and 1996, he was a research faculty at Lawrence Berkeley National Laboratory, Berkeley California. Dr Malluhi was the co-founder and CTO of Data Reliability Inc. (2001-2005). He was a co-Founder of the Qatar Cloud Computing Center (2009). He was the co-founder and executive advisor of the Qatar University Wireless Innovation Center at the Qatar Science and Technology Park (2008-2009). He served as a consultant for several telecommunication companies where he built networks, designed internet/intranet systems, developed distributed applications and telecommunication management software. Prof. Malluhi's research area is in the fields distributed systems, cloud computing, data security, high performance storage systems, and computer networks. His research efforts have been supported by grants and contracts from the Qatar National Research Fund, Lawrence Berkeley National Laboratory, the US Department of Energy, the National Science Foundation, NASA, the US Department of Defense, and IBM. Prof. Malluhi has received a number of honors and awards including the QU research award (2007), the JSU Technology Transfer and Entrepreneurship award (2004), the Mississippi University Research Authority support (2003), and the JSU faculty Excellence award (2001). Dr Qutaibah Malluhi has received M.S. and Ph.D. degrees in Computer Science from the Center of Advanced Computer Studies, University of Louisiana, Lafayette in 1993 and 1994, respectively. He also has B.S. and M.S. degrees, with honors in Computer Engineering from King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia in 1988 and 1990, respectively.

***Talk**: Cloud Computing without Seeing*

**Abstract:** Cloud computing is an emerging model in which applications, data, computing resources and operating platforms are provided to clients as a service. Despite its obvious benefits, cloud computing poses several trust and security challenges that can be serious impediments to its use. These security concerns include the risk of data breaches, malicious corruption of computation results, uncertainty about data privacy, and lack of client control on their data assets that are residing on third-party infrastructure. This talk discusses practical techniques that enable private outsourcing on the cloud by allowing the service provider to work on clients' data or computations without seeing the data being processed. These techniques would enhance the clients' trust in cloud computing and should be used to augment the reliance service level agreements. The talk focuses on two scenarios of outsourcing and

discusses solutions that are being developed through collaborative projects between Qatar University and Purdue University.

*Paper 5 by Boulares Ouchenne and Ousmane Koné*

*Specifying and Analysing Run-Time Security Policies for Time Dependant Services*

**Abstract:** We deal with the issue of specifying security policies that can be enforced by monitoring services execution. Currently, the vast majority of works focus on access control, are based on logics, and offer ways to express high level properties of real-time systems. However, the expressiveness power of such logics does not allow us to express recent usage control requirements (like accounting), and the undecidability of such logics hardens the task of analyzing and querying such security policies. Our work offers rather an operational approach, by the use of timed automata to specify and analyze security policies that can be enforced through mechanisms that work by monitoring the system execution. We show how to specify such complex policies as combinations of simpler modular policies. Then for a given set of policies, we suggest methods to analyze and establish whether this set of policies is consistent or not.

## Session 5

### Keynote 5 by Mazen Hamdan

**Bio:** Mr. Hamdan has 18 years of experience in central banking. He is currently heading the Cash Operations department at the Central Bank of Lebanon. Concurrently, he is also the youngest member of its Open Market Committee, the highest board at the bank for the design and formulation of the national monetary policy, headed by H.E the governor and including members such as vice-governors, senior management from the central bank and high government officials. For the past 4 years, and in record time, Mr. Hamdan has turned the Cash operations Department into a highly efficient, effective, and sophisticated operating center, with cutting-edge technology, and state-of-the-art innovations. Through restructuring and modernizing its systems and procedures, and while realigning the department's products and services within the overall strategy of the Central Bank, Mr. Hamdan was able to cut his department's costs dramatically, turning it into a profit center while at the same time increasing its scope of work. The restructuring allowed for a decrease the number of staff from 120 to 70 while at the same time doubling the daily turnover of deposited banknotes and has made the department a module and reference for other central banks. Before being assigned to this position, Mr. Hamdan was assistant Director at the Organization and Development department, where he initiated and implemented several projects for restructuring the processes and the systems at the central bank as a whole. During that time, and for seven years, Mr. Hamdan developed several practices and procedures, for audit and control, as well as risk management. Previously, Mr. Hamdan was responsible for the Mergers and Acquisitions Section at the Asset Management Department from the date he joined the central bank in 1993. Being exposed to different challenges, Mr. Hamdan has a rich and diverse experience in creating and managing innovative development projects. Mr. Hamdan has been a lecturer at the Lebanese University for several years, teaching Project Management. He is also a trainer and a resource person for the central bank's training program. Mr. Hamdan has a Business degree from the American University of Beirut, and a Masters Degree in Accounting and Finance from the London School of Economics and political Science.

*Talk: Banknotes Security Features*

**Abstract:** Document security in general and Banknote security features in particular have long been at the fore front of technological innovation. The levels of banknote security are directed to different target groups with varying degrees of complexity. This paper will demonstrate the Banque Du Liban's approach to the banknote security features and the basis for making those choices as well as other techniques used in document security.

*Paper 6 by Nashwa El-Bendary, Mostafa A. Salama and Aboul Ella Hassanien.*

*Towards Secure Mobile Agent Based E-Cash System*

**Abstract:** Electronic cash is a payment system that enables a secure off-line transaction without revealing the payers identity. Concerning anonymity of user, it may be misused for illegal purposes through cloning the signed code delivered to a client in order to be spent in multi-payment processes, which is called "double spending". Many proposed electronic payment schemes have failed to reach a solution to prevent the double spending problem. This paper presents a solution for the double spending problem during electronic cash payment phase via proposing a mobile agent based electronic cash system. This has been achieved through combining an Optical Memory Card with mobile agent technology that are presenting hardware and software, respectively.

## Student Session

*Visual Framework for XML Manipulation and Control*
*Gilbert Tekli*

**Abstract**: XML has spread beyond the computer science fields and reached other areas such as, e-commerce, identification, information storage, instant messaging and others. Data communicated over these domains is now mainly based on XML. Thus, allowing non-expert programmers to manipulate and control their XML data is essential. In the literature, this issue has been dealt with from 2 perspectives: (i) XML alteration/adaptation techniques requiring a certain level of expertise to be implemented and are not unified yet, and (ii) Mashups, which are not formally defined yet and are not specific to XML data, and XML-oriented visual languages are based on structural transformations and data extraction mainly and do not allow XML textual data manipulations. In this paper, we discuss existing approaches and present our XA2C framework intended for both non-expert and expert programmers and providing them with means to write/draw their XML data manipulation operations. The framework is defined based on the dataflow paradigm (visual diagram compositions) while taking advantage of both Mashups and XML-oriented visual languages by defining a well founded modular architecture and an XML-oriented visual functional composition language based on colored petri nets allowing functional compositions. The framework takes advantage of existing XML alteration/adaptation techniques by defining them as XML-oriented manipulation functions.

## *Inference Detection via Textual Annotations*
*Eliana Raad*

**Abstract:** With the growth of digital libraries and digital collections, elements such as images, videos, audios and texts became fully accessible. This open environment requires a balance between the need of open access against the need of data protection. The latter is a highly emphasized issue in today's business, where one of its aspects is to prevent the leakage of sensitive and protected *multimedia elements* (objects of interest in a video, images, etc.) during the access of digital documents. The problem is when published *multimedia elements*, combined with textual data description, allow unintended inferences leading to the identification of sensitive and confidential objects of interest. This problematic aspect arises needs related to addressing the text surrounding *multimedia elements* which includes captions, textual description or any text related to any object of interest in the *multimedia element*.

## *Privacy Preserving in a Video Database*
*Firas AL Khalil*

**Abstract**: Providing techniques to protect sensitive video content is a crucial need especially with the rapid growth of social networking websites where users publish frequently their related videos through services offered to their user-base. In a video element, privacy concerns related to information association present a real challenge to the research community due to the wide range of information that can be gathered from the video to form a source of inference. Here, we present a novel technique for privacy preserving in a video database. Our technique tackles possible data association established on the basis of speech segments, subtitles and other video embedded textual annotations leading to the identification of sensitive and protected objects of interest.

## *The Trust Platform*
*Helene Kovas & Roy Nohra*

**Abstract:** The lack of privacy control on social networks is becoming an increasingly alarming problem. Users are publishing all sorts of data from textual notes and annotations to images and videos revealing some intimate and sensitive information related to their lives and the lives of their friends and families. In essence, in such environment, users' privacy is somehow related to information published by others which in many situations is beyond his/her control and depends on the data holder's intentions. Here, we present a framework for privacy control using mutual agreements making every user on a social network a right holder with the ability to control at certain granularities information published by data holders (friends).